

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS

CHRISTINE BRYANT on behalf of herself)
and all other persons similarly situated, known)
and unknown,)
Plaintiff,) Case No. 1:19-cv-06622
vs.) Honorable Virginia M. Kendall
COMPASS GROUP USA, INC.)
Defendant.)

FIRST AMENDED CLASS ACTION COMPLAINT

Christine Bryant (“Plaintiff”), files this First Amended Class Action Complaint (“Complaint”) against Compass Group USA, Inc. (“Defendant”) for violations of the Illinois Biometric Information Privacy Act.

SUMMARY OF CLAIMS

1. Defendant is the nation's largest vending machine services company.
2. Among its services, Defendant provides Smart Market vending machines that a purchaser uses by scanning his or her fingerprint.
3. Defendant provides Smart Market vending machines to companies throughout Illinois.
4. Plaintiff was employed by Alorica, a call center, in Rockford, Illinois from approximately February 2018 to July 2018.
5. Defendant provided Alorica with Smart Market vending machines in the company's cafeteria.
6. During Plaintiff's orientation with Alorica, new employees were directed to go into the cafeteria and set up an account with Defendant's vending machines.

7. A representative of Defendant directed Plaintiff and other Alorica employees to scan their fingerprints into the Smart Market vending machine system to set up an account under their names.

8. As directed, Plaintiff and other Alorica employees scanned their fingerprints into Defendant's Smart Market vending machine system to set up their accounts.

9. Throughout her employment, Plaintiff regularly purchased items from Defendant's vending machines by scanning her fingerprint in the vending machines.

10. Plaintiff also scanned her fingerprint in Defendant's vending machines whenever she added money to a card Defendant gave her to fund her purchases.

11. Fingerprints are *unique* and *permanent* identifiers.

12. In enacting the Biometric Information Privacy Act, the Illinois legislature recognized that biologically unique identifiers, like fingerprints, can never be changed when compromised, and thus subject a victim of identity theft to heightened risk of loss.

13. As a result, Illinois restricted private entities, like Defendant, from collecting, storing, using, or transferring a person's biometric identifiers and information without adhering to strict informed-consent procedures established by the Biometric Information Privacy Act.

14. Defendant collected, stored, and used the unique biometric fingerprint identifiers, or information derived from those identifiers, of Plaintiff and others similarly situated without following the detailed requirements of the Biometric Information Privacy Act.

15. As a result, Plaintiff and others similarly situated lost the right to control their biometric identifiers and information.

JURISDICTION AND VENUE

16. This Court has personal jurisdiction over Defendant because, during the relevant

time period, Defendant did business in Illinois, was registered to do business in Illinois, and committed the statutory violations alleged in this Complaint in Illinois.

17. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d), because Plaintiff and Defendant are citizens of different states, there are over 1,000 potential class members, and there is over \$5,000,000 in controversy.

18. Venue is proper in the Northern District of Illinois pursuant to 29 U.S.C. § 1391(a)(2) because the events giving rise to this action took place here.

THE PARTIES

19. Plaintiff is an individual who is a citizen of Illinois.

20. Defendant is a Delaware corporation.

21. Defendant's principal place of business is in Charlotte, North Carolina.

REQUIREMENTS OF THE BIOMETRIC INFORMATION PRIVACY ACT

22. In enacting the Biometric Information Privacy Act, the Illinois legislature recognized that the full ramifications of biometric technology are not yet fully known and so the public will benefit from "regulations on the collection, use, safeguarding, handling, storage retention, and description of biometric identifiers and information." 740 ILCS 14/5(f)-(g).

23. The Biometric Information Privacy Act prohibits a "private entity" from capturing or collecting biometric identifiers or information from an individual unless that private entity first obtains the individual's written release authorizing the private entity to capture or collect an individual's biometric identifiers and/or biometric information. 740 ILCS 14/15(b)(3).

24. Relatedly, the Biometric Information Privacy Act prohibits a private entity from capturing or collecting biometric identifiers or information from an individual unless that private entity first informs the individual, in writing, of the following: (a) that the private entity is

collecting biometric identifiers or information, (b) the purpose of such collection, and (c) the length of time the private entity will retain the biometric identifiers or information. 740 ILCS 14/15(b)(1)(b).

25. In addition, the Biometric Information Privacy Act prohibits a private entity from possessing biometric identifiers or information unless it creates and follows a written policy, made available to the public, establishing a retention schedule and destruction guidelines for its possession of biometric identifiers and information; the private entity must destroy biometric identifiers and information once the purpose for collection has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever is sooner. 740 ILCS 14/15(a).

BACKGROUND FACTS

26. When Plaintiff scanned her fingerprint in Defendant's Smart Market vending machine system, Defendant captured and stored Plaintiff's fingerprint, or a representation derived from Plaintiff's fingerprint.

27. Defendant never provided Plaintiff any written materials stating that it was collecting, using, or retaining her fingerprint or a representation derived from her fingerprint.

28. Defendant never obtained Plaintiff's written release authorizing the collection, use, or storage of her fingerprint or a representation derived from Plaintiff's fingerprint.

29. Defendant did not timely destroy Plaintiff's fingerprint data once the purpose for collecting it was complete: once she separated her employment with Alorica.

CLASS ACTION ALLEGATIONS

30. Plaintiff seeks to represent a class of individuals who scanned their fingerprints in one or more of Defendant's vending machines in Illinois between August 23, 2014 and the present ("the Class").

31. Plaintiff and the Class are similar to one another because they were all subject to the same allegedly illegal practice: scanning their fingerprints in Defendant's biometric vending machines despite Defendant failing to adhere to the requirements of the Biometric Information Privacy Act.

32. The Class includes more than 50 members.

33. As a result, the Class is so numerous that joining of all class members in one lawsuit is not practical.

34. The issues involved in this lawsuit present common questions of law and fact, including: whether the Class scanned their fingerprints in Defendant's vending machines; whether Defendant collected the Class's "biometric identifiers" or "biometric information" under the Biometric Information Privacy Act; and whether Defendant complied with the procedures in 740 ILCS 14/15(a) and (b) of the Biometric Information Privacy Act.

35. These common questions of law and fact predominate over variations that may exist between members of the Class, if any.

36. Plaintiff, the members of the Class, and Defendant have a commonality of interest in the subject matter of the lawsuit and the remedy sought.

37. If individual actions were required to be brought by each member of the Class injured or affected, the result would be a multiplicity of actions, creating a hardship to the Class, to the Court, and to Defendant.

38. Accordingly, a class action is an appropriate method for the fair and efficient adjudication of this lawsuit and distribution of the common fund to which the Class is entitled.

39. The books and records of Defendant are material to Plaintiff's case as they disclose when Plaintiff and the Class scanned their fingerprints in Defendant's vending machines and what

information Defendant provided Plaintiff and the Class about the collection, retention, and use of their biometric identifiers and information.

40. Plaintiff and her counsel will fairly and adequately protect the interests of the Class.

41. Plaintiff retained counsel experienced in complex class action litigation.

COUNT I

Violation of the Biometric Information Privacy Act (740 ILCS 14/15(b))
(Class Action)

42. Plaintiff realleges and incorporates the previous allegations of this Complaint.

43. Defendant is a “private entity” under the Biometric Information Privacy Act. 740 ILCS 14/10.

44. Plaintiff’s and the Class’s fingerprints qualify as “biometric identifier[s]” as defined by the Biometric Information Privacy Act. 740 ILCS 14/10.

45. Defendant has “biometric information” from Plaintiff and the Class through its acquisition and retention of information based on Plaintiff’s and the Class’s fingerprints.

46. Defendant violated the Biometric Information Privacy Act by capturing or collecting Plaintiff’s and the Class’s fingerprints and information based on their fingerprints without first informing them in writing that Defendant was doing so.

47. Defendant violated the Biometric Information Privacy Act by capturing or collecting Plaintiff’s and the Class’s fingerprints and information based on their fingerprints without first informing them in writing of the purpose of Defendant doing so and the length of time Defendant would store and use Plaintiff’s and the Class’s biometric identifiers and/or biometric information.

48. Defendant violated the Biometric Information Privacy Act by capturing or collecting Plaintiff’s and the Class’s fingerprints and information based on their fingerprints

without first obtaining their written consent or other release authorizing Defendant to capture or collect Plaintiff's and the Class's biometric identifiers and/or biometric information.

49. Defendant knew or should have known of the requirements of the Biometric Information Privacy Act because the law was enacted in 2008 and numerous articles and court filings about the law's requirements were published before Defendant directed Plaintiff to scan her fingerprint into Defendant's vending machine system.

50. As a result, Defendant's violations of the Biometric Information Privacy Act were reckless or, in the alternative, negligent.

WHEREFORE, Plaintiff and the Class pray for a judgment against Defendant as follows:

- A. Awarding liquidated or actual monetary damages, whichever is higher, to Plaintiff and the Class for each violation of the Biometric Information Privacy Act as provided by 740 ILCS 14/20(1)-(2);
- B. Enjoining Defendant from committing further violations of the Biometric Information Privacy Act as authorized by 740 ILCS 14/20(4);
- C. Awarding Plaintiff's reasonable attorneys' fees and costs incurred in filing and prosecuting this action as provided by 740 ILCS 14/20(3); and
- D. Such other and further relief as this Court deems appropriate and just as provided by 740 ILCS 14/20(4).

COUNT II
Violation of the Biometric Information Privacy Act (740 ILCS 14/15(a))
(Class Action)

51. Plaintiff realleges and incorporates the previous allegations of this Complaint.

52. Defendant is a "private entity" under the Biometric Information Privacy Act. 740 ILCS 14/10.

53. Plaintiff's and the Class's fingerprints qualify as "biometric identifier[s]" as defined by the Biometric Information Privacy Act. 740 ILCS 14/10.

54. Defendant possessed “biometric information” from Plaintiff and the Class through its acquisition and retention of information based on Plaintiff’s and the Class’s fingerprints.

55. Defendant violated the Biometric Information Privacy Act by failing to timely destroy fingerprint data once the purpose for collecting that information was complete: once Plaintiff separated employment from Alorica.

56. Defendant knew or should have known of the requirements of the Biometric Information Privacy Act because the law was enacted in 2008 and numerous articles and court filings about the law’s requirements were published before Defendant directed Plaintiff to scan her fingerprint into Defendant’s vending machine system.

57. As a result, Defendant’s violations of the Biometric Information Privacy Act were reckless or, in the alternative, negligent.

WHEREFORE, Plaintiff and the Class pray for a judgment against Defendant as follows:

- A. Awarding liquidated or monetary damages, whichever is higher, to Plaintiff and the Class for each violation of the Biometric Information Privacy Act as provided by 740 ILCS 14/20(1)-(2);
- B. Enjoining Defendant from committing further violations of the Biometric Information Privacy Act as authorized by 740 ILCS 14/20(4);
- C. Awarding Plaintiff’s reasonable attorneys’ fees and costs incurred in filing and prosecuting this action as provided by 740 ILCS 14/20(3); and
- D. Such other and further relief as this Court deems appropriate and just as provided by 740 ILCS 14/20(4).

Respectfully submitted,

Dated: August 12, 2020

/s/ Douglas M. Werman
One of Plaintiff's Attorneys

Douglas M. Werman (dwerman@flsalaw.com)
Maureen A. Salas (msalas@flsalaw.com)
Zachary C. Flowerree (zflowerree@flsalaw.com)
Sarah J. Arendt (sarendt@flsalaw.com)
WERMAN SALAS P.C.
77 W. Washington Street, Suite 1402
Chicago, Illinois 60602
(312) 419-1008

Attorneys for Plaintiff